

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: S. FURUYA, et al
Serial No.: Not yet assigned
Filed: March 28, 2001
For: METHOD AND APPARATUS FOR SYMMETRIC-KEY
ENCRYPTION
Group: Not yet assigned
Examiner: Not yet assigned

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

March 28, 2001

Sir:

The following amendments and remarks are respectfully
submitted prior to the Rule 53(b) Continuation Application
filed on even date.

IN THE SPECIFICATION

Please insert before the first line of the specification
the following:

-- This is a Divisional Application of Serial No.
09/784,254, filed February 16, 2001. --

IN THE CLAIMS

Please cancel claims 1-8, 13-20, 25-32 and 37 without
prejudice or disclaimer of the subject matter thereof.

IN THE ABSTRACT

Please replace the Abstract of the invention with the attached new Abstract.

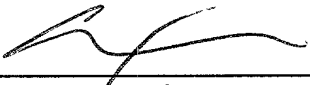
REMARKS

Entry of the above amendments prior to examination is respectfully requested.

Please charge any shortage in fees due in connection with the filing of this paper, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (520.39632VX1).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 312-6600

ABSTRACT

A symmetric-key cryptographic technique for realizing high-speed cryptographic processing, and alteration detection. The invention divides plaintext redundancy including data and a message to generate plural plaintext blocks each having a predetermined length, generates a random number sequence based on a secret key, generates a random number block corresponding to plaintext block from the random number sequence outputs a feedback value obtained from operation on the plaintext block and the random number block, the feedback value being fed back to another plaintext block, and performs an encryption operation using the plaintext block, the random number block, and a feedback value obtained from operation on another plaintext block to produce a ciphertext block.